WHAT IS CLAIMED IS:

1. A method of facilitating exchange of a key set (103) comprising one or more keys at a key access location, the method comprising:

scanning a key token attached to the key set (103) to obtain a unique key identifier; identifying the key access location; assigning the key set (103) to a bin (125, 502) at the key access location; and associating the bin (125, 502) and the key access location with the key identifier;

receiving an access rule for the key set (103) wherein the access rule identifies an authorized party (104);

publishing the key access location to the authorized party (104), preferably by sending the key access location to a user account or email account accessible by the authorized party (104);

receiving an access request for the key set (103) from the authorized party (104) through a client device (112), the access request providing user credentials;

authenticating the access request by verifying the user credentials provided in the access request against a set of credentials associated with the authorized party (104); and

if the access request is authenticated, transmitting an access instruction for presentation of the key set (103); wherein transmitting the access instruction comprises, for example, transmitting the bin (125, 502) associated with the key set (103) to the client device (112), or transmitting a signal to a control and processing unit (122, 510) controlling the bin (125, 502) to cause the key set (103) to be made accessible such as by unlocking the bin (125, 502).

2. The method according to claim 1 wherein authenticating the access request further comprises comparing an identified location of the authorized party (104) with the key access location associated with the key identifier, wherein identifying the location of the authorized party (104) is preferably based on a location of the client device (112) wherein determining the location of the client device (112) comprises receiving from the client device (112) one or more of: GPS data, mobile network location data, device identity data, a physical interaction with the device (112), and user data input.

3. The method according to one of claims 1 or 2 wherein the access rule comprises an authorized access period, the method comprising identifying a time of the access request and authenticating the access request comprises comparing the time of the access request with the authorized access period.

4. The method according to any one of claims 1 to 3 comprising receiving a plurality of access rules for the key set (103), wherein each one of the access rules identifies an authorized party (104) and a corresponding authorized access period, and publishing the key access location to each one of the authorized parties (104).

5. The method according to claims 1 to 4 comprising automatically generating one or more access rules for the key set (103) in response to one or more of: a user request for a service in a home, a property booking, a recurring access request, and a request by a third party system authorized to make requests of the key exchange service.

6. The method according to any one of claims 1 to 5 verifying receipt or presentation of a valid key set (103) by initiating a scan of the key token at the key access location to read the key identifier of the key set (103) from the key token so it may be evaluated by the key exchange server (108), and preferably periodically scanning key tokens of key sets (103) at one or more key exchange locations and updating the associations of key identifiers with bins (125, 502) and the key access locations based on the information from the periodic scans.

7. The method according to any one of claims 1 to 6 wherein the key identifier is encoded on the keychain (103A, 400) attached to the key set (103), such as in an NFC tag (406).

8. The method according to any one of claims 1 to 7 automatically generating a notification to a user associated with the key set (103) in response to one or more of:

the key set (103) being presented to the authorized party (104);

the key set (103) being dropped off at a key access location;

the key set (103) not being presented to the authorized party (104) by a specified time; and

lapse of a predetermined period of time prior to expiry of the access period;

wherein the notification to the authorized party (104) preferably includes the option for content to be included by an administrative user associated with the key set (103).

9. A system for facilitating asynchronous exchange of a key set (103) comprising one or more keys at one of a plurality of key access locations, the system comprising a key exchange server (108) configured to:

receive a unique key identifier encoded on a key token attached to the key, wherein the key token is preferably located on a keychain (103A, 400) attached to the key set (103);

determine the key access location;

assign to the key set (103) a bin (125, 502) at the key access location;

associate the bin (125, 502) and the key access location with the key identifier;

receive or generate an access rule for the key set (103), wherein the access rule identifies an authorized party (104);

publish the key access location to the authorized party (104), preferably by sending the key access location to a user account or email account accessible by the authorized party (104);

receive an access request for the key set (103) from the authorized party (104) through a client device (112), the access request providing user credentials;

authenticate the access request by verifying the user credentials provided in the access request against a set of credentials associated with the authorized party (104); and

if the access request is authenticated, transmit an access instruction for presentation of the key set (103) to the authorized party (104).

10. The system according to claim 9 wherein the key exchange server (108) is configured to: authenticate the access request by comparing an identified location of the authorized party (104) with the key access location associated with the key identifier, wherein the location of the authorized party (104) is preferably identified based on a location of the client device (112) wherein the location of the client device (112) is determined by receiving from the client device

(112) one or more of: GPS data, mobile network location data, device identity data, a physical interaction with the device (112), and user data input.

11. The system according to either of claims 9 and 10 wherein the access rule comprises an authorized access period and the key exchange server (108) is configured to identify a time of the access request and to authenticate the access request by steps comprising comparing the time of the access request with the authorized access period.

12. The system according to any one of claims 9 to 11 wherein the key exchange server (108) is configured to receive or generate a plurality of access rules for the key set (103), wherein each one of the access rules identifies an authorized party (104) and a corresponding authorized access period, and wherein the key exchange server (108) is configured to publish the key access location to each one of the authorized parties (104).

13. The system according to any one of claims 9 to 12 wherein the key exchange server is configured to generate access rules from system requests following one or more of: a user request for a service in a home, a property booking, a recurring access request, and a request by a third party system authorized to make requests of the key exchange server (108).

14. The system according to any one of claims 9 to 13 comprising a key cabinet subsystem (120, 500) comprising a plurality of bins (125, 502) at the key access location, wherein each one of the plurality of bins (125, 502) is preferably adapted to receive one key and keychain combination.

15. The system according to claim 14 wherein the key cabinet subsystem (120, 500) comprises a control and processing unit (122, 510) and the key exchange server (108) is configured to transmit an access instruction for presentation of the key set (103) by transmitting a signal to the control and processing unit (122, 510) to cause the key set (103) to be made accessible to the authorized party (104), and wherein the key cabinet subsystem (120, 500) further preferably comprises a scanner (514) in the bin (125, 502) and the key exchange server (108) is configured to transmit a signal to the control and processing unit (122, 510) causing the scanner (514) to be activated to read the key identifier of the key set (103) to verify that the requested key set (103) is in the bin (125, 502), wherein the key exchange server (108) is

preferably configured to periodically trigger scanning of key tokens of key sets (103) at one or more key exchange locations and to update the associations of key identifiers with bins (125, 502) and the key access locations based on the information from the periodic scans.

16. The system according to any one of claims 10 to 15 wherein the key exchange server (108) is configured to receive the key identifier from a scan of the key set (103) and to verify from the key identifier that the key set (103) to be received from or presented to the authorized party (104) is a valid key set (103).

17. The system according to any one of claims 10 to 15 wherein the key exchange server (108) is configured to transmit an access instruction for presentation of the key by transmitting the bin (125, 502) associated with the key set (103) to the client device (112).

18. The system according to any one of claims 10 to 17 wherein the key identifier associated with the key set (103) is linked to unique identification information visible on a key chain.

19. The system according to any one of claims 10 to 18 wherein the key identifier is encoded in an NFC tag (406) wherein the NFC tag (406) is preferably embedded in a recess (404) in a metal keychain (402) and is separated from the metal keychain (402) by an anti-metal layer (408) and is secured in the recess (404) by material for protecting and preserving the NFC tag such as an epoxy or plastic layer (410).

20. The system according to any one of claims 10 to 19 wherein the key exchange server (108) is configured to process a plurality of access rules for the key set (103), wherein each one of the access rules identifies an authorized party (104) and a corresponding authorized access period and wherein the key exchange server (108) is configured to publish the key access location to each one of the authorized parties (104).

21. The system according to either of claims 14 and 15 wherein the key exchange server (108) is configured to cause an interface application to be downloaded to the key cabinet subsystem (120, 500), the interface application comprising instructions for enabling the key cabinet subsystem (120, 500) to interface with the key exchange server (108) wherein the key exchange server (108) is preferably configured to cause updates to the interface application to be

downloaded to the key cabinet subsystem (120, 500) and/or to monitor a status of the key cabinet subsystem (120, 500).